IB/105/00828

PA 1301562

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 01, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *10/823,378* ✓
FILING DATE: *April 12, 2004* ✓

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

L. Edelen

L. EDELEN
Certifying Officer

14230 U.S.PTO

22387 U.S.PTO 10/823378 041204

PTO/SB/05 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	08212/0200353-US0
First Inventor	Adam Cain
Title	SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES
Express Mail Label No.	EV398895255US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

1. [X] Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original, and a duplicate for fee processing)*
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [X] Specification [Total Pages 17]
   (preferred arrangement set forth below)
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. [X] Drawing(s) *(35 U.S.C. 113)* [Total Sheets 6]
5. Oath or Declaration [Total Sheets 5]
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [X] Application Data Sheet. See 37 CFR 1.76
7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or ii. [ ] Paper
   c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. [X] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [ ] Power of Attorney
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [ ] Preliminary Amendment
14. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. [X] Other: Certificate of Express Mailing (1 page)
    Check for $40.00 for Assignment Recordation Only (1)

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: _____

Prior application information: Examiner _____ *Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

[X] Customer Number: 38879 OR [ ] Correspondence address below

Name	DARBY & DARBY P.C. Jamie L. Wiegand				
Address	P.O. Box 5257				
City	New York	State	NY	Zip Code	10150-5257
Country	US	Telephone	(206) 262-8900	Fax	(212) 753-6237

Name (Print/Type)	Jamie L. Wiegand	Registration No. (Attorney/Agent)	52,361
Signature	JLWiegand	Date	April 12, 2004

{S:\8212\0200353-US0\80006119.DOC [redacted]}

PTO/SB/17 (10-03)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 40.00

Complete if Known	
Application Number	Not Yet Assigned
Filing Date	Concurrently Herewith
First Named Inventor	Adam Cain
Examiner Name	Not Yet Assigned
Art Unit	N/A
Attorney Docket No.	08212/0200353-US0

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number: 04-0100

Deposit Account Name: Darby & Darby P.C.

The Director is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☐ Charge any additional fee(s) or any underpayment of fee(s)

☒ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below	=	Fee Paid
Total Claims	14	-20** =		x		=	0.00
Independent Claims	3	-3** =		x		=	0.00
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	43	Independent claims in excess of 3
1203	280	2203	145	Multiple dependent claim, if not paid
1204	88	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge – late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Jamie L. Wiegand	*Registration No. (Attorney/Agent)*	52,361	*Telephone*	(206) 262-8900
Signature	Jwiegand			*Date*	April 12, 2004

{S:\8212\0200353-US0\80006120.DOC}

Application No. (if known): Not Yet Assigned | Attorney Docket No.: 08212/0200353-US0

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV398895255US in an envelope addressed to:

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on April 12, 2004
Date

Signature

Jamie L. Wiegand
Typed or printed name of person signing Certificate

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Check for $40.00 for Assignment Recordation Only (1)
Return Receipt Postcard (1)
Certificate of Express Mailing (1 page)
Utility Patent Application Transmittal (1 page)
Fee Transmittal (1 page)
Utility Application (Inc. Spec., Claims and Abstract) (17 pages)
6 drawings (6 sheets)
Oath or declaration (5 pages)
Assignment Recordation Sheet (1 page)
Assignment (3 pages)
Application Data Sheet (3 pages)

Application Filing Fee Not Being Paid At This Time

{S:\8212\0200353-us0\80006118.DOC [redacted]}

D&D No. 08212/0200353-US0

SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES

Field of the Invention

The present invention relates to computer security, and in particular, to a system and method for authorizing access to a resource over a network using an attribute certificate.

Background

Earlier attempts to associate different authorization-related attributes to clients often relied on the client IP address as a means to identify the client. However, this technique proved not to be very effective, since the IP address of a network device may easily be changed. Furthermore, proliferation of Network Address Translation (NAT) devices and Virtual Private Networks (VPNs) makes it difficult for an access server to identify a particular client solely based on the client's IP address.

Commonly used Kerberos tickets provide a means for applications to share a cryptographically authenticated credential among several applications. However, Kerberos tickets only indicate that a particular user has successfully authenticated to a central network server, thereby establishing a single user session. Kerberos tickets do not convey user capabilities and they do not span multiple user sessions.

The use of hardware tokens for authentication addresses a related need. A hardware token allows a user to prove its identity as well as its possession of a particular physical object. In return, those proven assertions may lead to an expanded access right for a network service. However, a hardware token also does not provide a general means to convey user capabilities of the client.

Thus, it is with respect to these considerations and others that the present invention has been made.

Brief Description of the Drawings

Non-limiting and non-exhaustive embodiments of the present invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

For a better understanding of the present invention, reference will be made to the following Detailed Description of the Invention, which is to be read in association with the accompanying drawings, wherein:

FIGURE 1 illustrates one embodiment of an environment in which the invention operates;

FIGURE 2 illustrates a functional block diagram of one embodiment of a network device that may be configured to operate as a client;

FIGURE 3 illustrates a flow diagram generally showing one embodiment of a process for using an attribute certificate to authorize a client;

FIGURE 4 illustrates message flows involved in one embodiment of the present invention;

FIGURE 5 illustrates message flows involved in another embodiment of the present invention; and

FIGURE 6 illustrates message flows involved in yet another embodiment of the present invention.

Detailed Description of the Preferred Embodiment

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific exemplary embodiments by which the invention may be practiced. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Among other things, the present invention may be embodied as methods or devices. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely

software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

The terms "comprising," "including," "containing," "having," and "characterized by," refers to an open-ended or inclusive transitional construct and does not exclude additional, unrecited elements, or method steps. For example, a combination that comprises A and B elements, also reads on a combination of A, B, and C elements.

The meaning of "a," "an," and "the" include plural references. The meaning of "in" includes "in" and "on." Additionally, a reference to the singular includes a reference to the plural unless otherwise stated or is inconsistent with the disclosure herein.

The term "or" is an inclusive "or" operator, and includes the term "and/or," unless the context clearly dictates otherwise.

The phrase "in one embodiment," as used herein does not necessarily refer to the same embodiment, although it may.

The term "based on" is not exclusive and provides for being based on additional factors not described, unless the context clearly dictates otherwise.

The term "flow" includes a flow of packets through a network. The term "connection" refers to a flow or flows of messages that typically share a common source and destination.

Briefly stated, the present invention is directed to a method and system for authorizing a network device using attribute certificates.

Different network access capabilities may be provided to a user depending on properties of the user and device used to access the network. The invention may provide a secure way for the user to demonstrate that it has been approved for access to the network. An Attribute Certificate (AC) may be a digitally signed assertion including information about capabilities, restrictions, and the like, of the user and/or the device used to access the network. If the Attribute Certificate is issued upon completion of an automated security scan of a client device, the AC may be employed to provide a secure way for the device to inform an access server of the client

automated security scan results at a later time. If the AC is generated based on capabilities of the user, it provides the access server secure information needed to make network resources available to the user, based on the AC.

The AC may be issued to a user, which may present it to the access server from different client network devices. The AC may also be issued to a client network device, through which different users may access the same resource.

Illustrative Operating Environment

FIGURE 1 illustrates one embodiment of an environment in which a system may operate. Not all the components may be required to practice the invention, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the invention.

As shown in the figure, system 100 includes Local Area Network / Wide Area Network (LAN/WAN) 104, client 102, access server 106, attribute authority 108, and attribute repository 110. Client 102 and access server 106 are in communication over LAN/WAN 104. Access server 106 is in further communication with attribute authority 108 and attribute repository 110. Attribute authority 108 and attribute repository 110 are also in communication with each other.

LAN/WAN 104 is enabled to employ any form of computer readable media for communicating information from one electronic device to another. In addition, LAN/WAN 104 may include the Internet in addition to local area networks, wide area networks, direct channels, such as through a universal serial bus (USB) port, other forms of computer-readable media, and any combination thereof. On an interconnected set of LANs, including those based on differing architectures and protocols, a router acts as a link between LAN's, enabling messages to be sent from one to another. Also, communication links within LANs typically include twisted pair or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links including satellite links, or other communications links known to those

skilled in the art. Furthermore, remote computers and other related electronic devices may be remotely connected to either LANs or WANs via a modem and temporary telephone link. In essence LAN/WAN 104 may include any communication mechanism by which information may travel between network devices, such as client 102 and access server 106.

Client 102 may be any network device capable of communicating over a network, such as LAN/WAN 104, to access server 106, and the like. The set of such devices may include devices that typically connect using a wired communications medium such as personal computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, and the like, that are configured to operate as a network device. The set of such devices may also include devices that typically connect using a wireless communications medium such as cell phones, smart phones, pagers, walkie talkies, radio frequency (RF) devices, infrared (IR) devices, CBs, integrated devices combining one or more of the preceding devices, and the like, that are configured as a network appliance. Alternatively, client 102 may be any device that is capable of connecting using a wired or wireless communication medium such as a PDA, POCKET PC, wearable computer, and any other device that is equipped to communicate over a wired and/or wireless communication medium, operating as a network device. As such client 102 may be configured to operate as a web server, cache server, file server, router, file storage device, gateway, switch, bridge, firewall, proxy, and the like.

Access server 106 may include any computing device or devices capable to provide authorization to a resource over LAN/WAN 104. Devices seeking access to the resource over the network, such as client 102 may be authorized by access server 106 using an attribute certificate. Devices that may operate as access server 106 include, but are not limited to, personal computers, desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, web servers, cache servers, file servers, routers, gateways, switches, bridges, firewalls, proxies, and the like. The resource over the network may be any network service available to network devices connected to the network, such as client 102.

Attribute authority 108 includes any computing device or devices capable to determine an attribute of a network device seeking authorization such as client 102. Attribute authority 108 may further include network devices that verify an attribute of a network device such as client 102. Attribute authority 108 may also be configured to operate as a web server, cache server, file server, router, file storage device, gateway, switch, bridge, firewall, proxy, and the like. In one embodiment attribute authority 108 and access server 106 may reside in one computing device.

Attribute repository 110 may include any computing device or devices capable of receiving an attribute certificate from access server 106, attribute authority 108, and the like, and maintaining the attribute certificate ready for distribution. Devices that may operate as attribute repository 110 include, but are not limited to, personal computers, desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, servers, and the like. Attribute repository 110 may also include a web service, an FTP service, an LDAP service, and the like, configured to manage the attribute certificate, and related information. In one embodiment, attribute repository 110 may include a storage structure for maintaining trust information, such as public keys, signatures, access control lists, revocation lists, and the like. Attribute repository 110 may include subscription information, observer mechanisms, and the like, that enable a network device, such as access server 106, and the like, to monitor an availability of the attribute certificate, and associated information.

Although not shown, attribute authority 108 and attribute repository 110 may also be in direct communication with client 102.

FIGURE 2 illustrates a functional block diagram of one embodiment of network device 200 in which the present invention may be practiced. Network device 200 provides one embodiment for access server 106 of FIGURE 1. It will be appreciated that not all components of network device 200 are illustrated, and that network device 200 may include more or less components than those shown in the figure. Network device 200 may operate, for example, as a personal computer, a desktop computer, a multiprocessor system, a microprocessor-based or programmable

consumer electronic, a network PC, a web server, a cache server, a file server, a router, a gateway, a switch, a bridge, a firewall, a proxy, and the like. The communications may take place over a network, such as LAN/WAN 104 in FIGURE 1, the Internet, or some other communications network.

As illustrated in FIGURE 2, network device 200 includes central processing unit (CPU) 212, video display adapter 214, read only memory (ROM) 232, random access memory (RAM) 216, hard disk drive 228, input/output interface (I/O) 224, a CD-ROM/DVD-ROM drive 226, and a network interface unit 210 interconnected via a bus 222.

RAM 216, ROM 232, CD-ROM/DVD-ROM drive 226, and hard disk drive 228 are computer storage media, which may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can store the information and that can be accessed by a computing device.

Network interface unit 210 is constructed for use with various communication protocols including the TCP/IP and UDP/IP protocol. Network interface unit 210 may include or interface with circuitry and components for transmitting packets, and the like, over a wired and/or wireless communications medium. Network interface unit 210 is sometimes referred to as a transceiver, Network Interface Card (NIC), and the like. Network device 200 may also include an I/O interface 224 for communicating with external devices or users.

RAM 216 is generally interconnected with ROM 232 and one or more permanent mass storage devices, such as hard disk drive 228. RAM 216 stores operating system 220 for controlling the operation of network device 200. The operating system 220 may comprise an operating system such as UNIX, LINUX™, Windows™, and the like.

In one embodiment, RAM 216 stores program code for application software 250, authorization protocol 240, and Attribute Certificate (AC) evaluation protocol 242, and the like, for performing authorization functions of network device 200. Application software 250 may include any computer program. Authorization protocol 240 is directed to controlling access to a network resource as described in FIGURE 3. AC evaluation protocol 242 may be a complementary protocol that enables the authorization protocol 240 to evaluate an attribute of a network device, such as client 102 of FIGURE 1, desiring access to the resource over the network. The attribute may be based, in part, on a capability of client 102, a condition to be satisfied for another attribute to be valid, a result of an automated security scan, and the like.

General Operation

FIGURE 3 illustrates a flow diagram generally showing process 300 for authorizing a network device using attribute certificates, according to one embodiment of the invention. Process 300 may, for example, be implemented in access server 106 of FIGURE 1.

As shown in FIGURE 3, process 300 begins, after a start block, at block 302, where an attribute of the network device desiring authorization, such as client 102 of FIGURE 1, is determined. The attribute may be based, in part, on a capability or characteristic of the network device. For example, the network device may be a laptop issued to a particular user, and the like. In this example, the attribute may be based, in part, on the status of security software running on the network device, and the like.

The attribute, determined at block 302, may also be based, in part, on a condition to be satisfied for another attribute to be valid. In the above example, the primary attribute may be the assertion that the network device has an anti-virus software installed. The other attribute may be based, in part, on a condition that the anti-virus software is running on the network device, and the antivirus software is configured with virus definitions that are no more than 5 days old, as a further example.

In another embodiment, the attribute, determined at block 302 may further be based, in part, on a status of the network device desiring authorization, such

as a result of an automated security scan. For security reasons, an automated security scan of the network device may be performed and the result associated with the AC. Associating an automated security scan with the AC may eliminate the need to perform repeated automated security scans every time the network device requests authorization, since the AC may provide evidence of a recent automated security scan. Upon determination of the attribute to be associated with the AC, process 300 proceeds to block 304.

At block 304, the AC is generated based, in part, on the attribute determined at block 302. The AC may be generated by the device performing the authorization, such as access server 106 of FIGURE 1, the network device itself, a third party network device, such as the attribute authority 108 of FIGURE 1, and the like.

Processing then proceeds to block 306 of FIGURE 3, where the AC is stored. The storage may also be performed by the device performing the authorization, such as access server 106 of FIGURE 1, the network device itself, a third party network device, such as the attribute authority 108 of FIGURE 1, and the like. Upon completion of block 306, process 300 may wait until a request for authorization is received at block 308.

At block 308, the network device presents the authorizing device with a request for authorization. Although not shown, block 308 may include actions by the authorizing device including, but not limited to, retrieving the AC from the network device, a storage device, an external storage database, and the like.

Process 300 flows to block 310, where a decision is made, to determine whether the network device is authenticated for connection to the network. If authentication is verified, processing proceeds to decision block 312. If authentication is not verified, processing proceeds to block 316, where communication is terminated. Processing may then return to a calling process to perform other actions.

At block 312, the validity of the AC is determined. In determining the validity of the AC a number of factors may be used including, but not limited to, valid date range of the AC, device identifier recorded in the AC, digital signature, and the like. If the AC is valid, process 300 proceeds to block 314, where the network device is

authorized. If the AC is not valid, processing proceeds to block 316, where communication is terminated. Processing may then return to a calling process to perform other actions.

It will be understood that each block of the flowchart illustrations discussed above, and combinations of blocks in the flowchart illustrations above, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer-implemented process such that the instructions, which execute on the processor, provide steps for implementing the actions specified in the flowchart block or blocks.

Although the invention is described in terms of communication between a network device and an access server, the invention is not so limited. For example, the communication may be between virtually any resource, including but not limited to multiple clients, multiple servers, and any other device, without departing from the scope of the invention.

Accordingly, blocks of the flowchart illustrations support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustrations, and combinations of blocks in the flowchart illustrations, can be implemented by special purpose hardware-based systems, which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

Illustrative Embodiments

FIGURE 4 illustrates one embodiment of a message flow diagram for a system similar to the system shown in FIGURE 1. As shown in the diagram, message flow 400 includes network resource 402, attribute repository 404, access server 406,

and client 408 across the top. Client 408 and access server 406 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

As shown in FIGURE 4, the message flows are divided into two groups separated by timeline 410. The first group comprises message flows involved in generating and storing an AC. This process may be repeated, if client 408 desires to store a certificate with a new access server, the stored AC is no longer valid for any of a variety of reasons, and the like. The process begins with access server 406 determining an attribute of client 408 to be associated with the AC. The attribute may be based, in part, on a capability of client 408. For example, client 408 may be a network device used by a user possessing temporary approval to utilize print services provided by a network resource. In this example, access server 406 may verify the printing capability approval for the network resource as the attribute to be associated with the AC.

Access server 406 may then generate the AC based, in part, on the attribute determined above. Following generation of the AC, access server 406 may send the AC to attribute repository 404, where the AC is stored.

The authorization process, as shown below timeline 410, in FIGURE 4, is typically started by receiving of a request for authorization from client 408. Upon receiving the request for authorization from client 408, access server 406 authenticates client 408. Authentication may be based on a login password, a digital certificate, a biometric parameter, and the like.

Upon authentication, access server 406 requests the AC from attribute repository 404. Attribute repository 404 sends the AC to access server 406, which verifies the AC's validity. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital signature on the AC, comparison of the identity listed in the AC with the authenticated identity of client 408, and the like.

If the AC is valid, access server 406 authorizes client 408 based, in part, on the attribute associated with the AC. Further using the example above, the

authorization provides client 408 with access to printing capabilities of network resource 402 based, in part, on the attribute associated with the AC.

FIGURE 5 illustrates a message flow diagram for a network system in accordance with another embodiment of the present invention. As shown in the diagram, message flow 500 includes network resource 502, access server 504, and client 506 across the top. Client 506 and access server 504 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

As shown in FIGURE 5, the message flows are divided into two groups separated by timeline 508. The first group comprises message flows involved in generating and storing an AC. The first part of the process is substantially similar to the first process described in FIGURE 4, above timeline 410. One difference between the two processes is access server 504 sends the AC to client 506 instead of an attribute repository, and client 506 stores the AC.

The authorization process, as shown below timeline 508, in FIGURE 5, is typically started by receiving of a request for authorization from client 506. Upon receiving the request for authorization from client 506, access server 504 authenticates client 506. Authentication may be based on a login password, a digital certificate, a biometric parameter, and the like.

Upon authentication, access server 504 verifies that the client is in possession of a valid AC. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital signature on the AC, comparison of the identity listed in the AC with the authenticated identity of client 506, and the like.

If the AC is valid, access server 504 authorizes client 506 based, in part, on the attribute associated with the AC. Using the example described in FIGURE 4 above, the authorization provides client 506 with access to printing capabilities of network resource 502 based, in part, on the attribute associated with the AC.

FIGURE 6 illustrates a message flow diagram for a network system in accordance with a further embodiment of the present invention. As shown in the

diagram, message flow 600 includes access server 602, client 604, and attribute authority 606 across the top. Client 604 and access server 602 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

As shown in FIGURE 6, the message flows are divided into two groups separated by timeline 608. The first group comprises message flows involved in generating and storing an AC. The process begins with an automated security scan of client 604 performed by attribute authority 606. Attribute authority 606 generates the AC based, in part, on a result of the automated security scan of client 604, and stores the AC.

The authorization process, as shown below timeline 608, in FIGURE 6, is typically started by receiving of a request for authorization from client 604. Upon receiving the request for authorization from client 604, access server 602 authenticates client 604. Authentication may be based on a login password, a digital certificate, a biometric parameter, and the like.

Upon authentication, access server 602 requests the AC from attribute authority 606. Attribute authority 606 send the AC to access server 602, which verifies the validity of the AC. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital signature on the AC, and the like.

If the AC is valid, access server 602 authorizes client 604 based, in part, on the attribute associated with the AC. In this embodiment, the authorization provides client 604 with access to network resources.

The above specification, examples, and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WE CLAIM:

1. A method for authorizing a network device, comprising:

determining an attribute based, in part, on a capability of the network device;

generating an attribute certificate based, in part, on the attribute;

storing the attribute certificate including the attribute; and

if the attribute certificate is valid, authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.

2. The method of Claim 1, wherein the attribute is further determined based, in part, on an automated security scan of the network device.

3. The method of Claim 1, wherein the attribute is further determined based, in part, on a condition to be satisfied.

4. The method of Claim 1, wherein the attribute is further associated with a group of network devices.

5. The method of Claim 1, wherein the attribute is further associated with a group of users.

6. The method of Claim 1, wherein the attribute certificate is generated by at least one of the network device, an access server, and an attribute authority.

7. The method of Claim 1, wherein the attribute certificate is stored in at least one of the network device, and an attribute repository.

8. The method of Claim 7, wherein the attribute certificate is provided to an access server through the use of at least one of a cookie, a program, and a manual upload.

9. A network device for managing authorization to a resource over a network, comprising:

a first component configured to generate an attribute certificate, wherein the attribute certificate is based, in part, on a capability of another network device;

a second component, coupled to the first component, configured to store the attribute certificate; and

a third component, coupled to the second component, configured to authorize the other network device to the resource over the network based, in part, on the attribute of the other network device associated with the attribute certificate.

10. The network device of Claim 9, wherein the first component is further configured to generate the attribute certificate based on a condition to be satisfied.

11. The network device of Claim 9 further comprising a fourth component that is configured to perform an automated security scan of the other network device.

12. The network device of Claim 11, wherein the first component is further configured to generate the attribute certificate based on the automated security scan of the other network device.

13. The network device of Claim 9, wherein the second component is further configured to send the attribute certificate to the other network device to be stored, and the third component it further configured to receive the attribute certificate.

14. A network device for managing authorization to a resource over a network, comprising:

a means for generating an attribute certificate, wherein the attribute certificate is based on a capability of another network device;

a means for storing the attribute certificate; and

a means for authorizing the other network device to the resource over the network based, in part, on the attribute of the other network device associated with the attribute certificate.

Abstract

Methods and devices are directed to authorizing a network device to a resource over a network. An access server determines based, in part, on an attribute of the network device associated with the attribute certificate, whether the network device may be authorized access to the resource over the network. The attribute may be associated with a capability granted to the network device, a condition to be satisfied for the attribute to be valid, and the like. The attribute may belong to a group of network devices, or one or more users accessing the network through the network device. In one embodiment, the attribute certificate may be provided based on an automated security scan of the network device. In another embodiment, the access server may make the attribute available to a network resource associated with the access server.

Customer No. 38879

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is described and claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES

the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to herein. I do not know and do not believe that the same was ever known or used in the United States of America before my or our invention thereof or patented or described in any printed publication in any country before my or our invention thereof, or more than one year prior to this application, or in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigned more than twelve months prior to this application.

I acknowledge the duty to disclose all information known to me that is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56.

FOREIGN PRIORITY CLAIM

I hereby claim foreign priority benefits under Title 35, United States Code § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

[x] no such foreign applications have been filed

[ ] such foreign application have been filed as follows:

EARLIEST FOREIGN APPLICATION(S), IF ANY FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

Application Number	Country	Date of Filing	Priority Claimed Under 35 USC 119
			___ Yes No ___
			___ Yes No ___
			___ Yes No ___

ALL FOREIGN APPLICATION(S), IF ANY FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

Application Number	Country	Date of Filing

CLAIM FOR BENEFIT OF EARLIER U.S. PROVISIONAL APPLICATIONS

I hereby claim priority benefits under Title 35, United States Code §119(e), of any United States provisional patent application(s) listed below:

[x] no such U.S. provisional applications have been filed.

[ ] such U.S. provisional application have been filed as follows:

Application Number	Date of Filing	Priority Claimed Under 35 USC 119
		___ Yes No ___
		___ Yes No ___
		___ Yes No ___

CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S)

I hereby claim the benefit under Title 35, United States Code, §120 of the United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information that is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56 which became available to me between the filing date of the prior application and the national or PCT international filing date of this application:

[x] no such U.S./PCT applications have been filed.

[ ] such U.S./PCT application have been filed as follows:

Application Number	Date of Filing	Status (Patented/Pending/Abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the practitioners under Customer Number

38879

all of **Darby & Darby P.C.**, P.O. Box 5257, New York, New York 10150-5257, jointly, and each of them severally, my attorneys at law/patent agent(s), with full power of substitution, delegation and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, and to transact all business in the U. S. Patent and Trademark Office connected therewith.

Please mail all correspondence to Jamie L. Wiegand, whose address is:

Darby & Darby P.C.
P.O. Box 5257
New York, New York 10150-5257

Please direct telephone calls to: Jamie L. Wiegand at (206) 262-8915.

Please direct facsimiles to: (212) 753-6237

Attorney Docket No.: 08212/0200353-US0

Full name of third inventor, if any	
Adam Cain	
Third inventor's signature	Date 3/7/04
Residence	
Madison, Wisconsin	
Citizenship US	
Mailing Address	
461 N. Few St. Madison, Wisconsin 53703	

Full name of sole or first inventor	
Craig R. Watkins	
Sole or first inventor's signature	Date
Residence	
State College, Pennsylvania	
Citizenship US	
Mailing Address	
1883 Huntington Lane State College, Pennsylvania 16803-3346	

Full name of second inventor, if any	
Jeremey Barrett	
Second inventor's signature	Date
Residence	
Sugar Land, Texas	
Citizenship US	
Mailing Address	
3330 Big Horn Ct. Sugar Land, Texas 77478	

Full name of third inventor, if any Adam Cain	
Third inventor's signature	Date
Residence Madison, Wisconsin	
Citizenship US	
Mailing Address 461 N. Few St. Madison, Wisconsin 53703	

Full name of sole or first inventor Craig R. Watkins	
Sole or first inventor's signature	Date 20 Feb 2004
Residence State College, Pennsylvania	
Citizenship US	
Mailing Address 1883 Huntington Lane State College, Pennsylvania 16803-3346	

Full name of second inventor, if any Jeremey Barrett	
Second inventor's signature	Date
Residence Sugar Land, Texas	
Citizenship US	
Mailing Address 3330 Big Horn Ct. Sugar Land, Texas 77478	

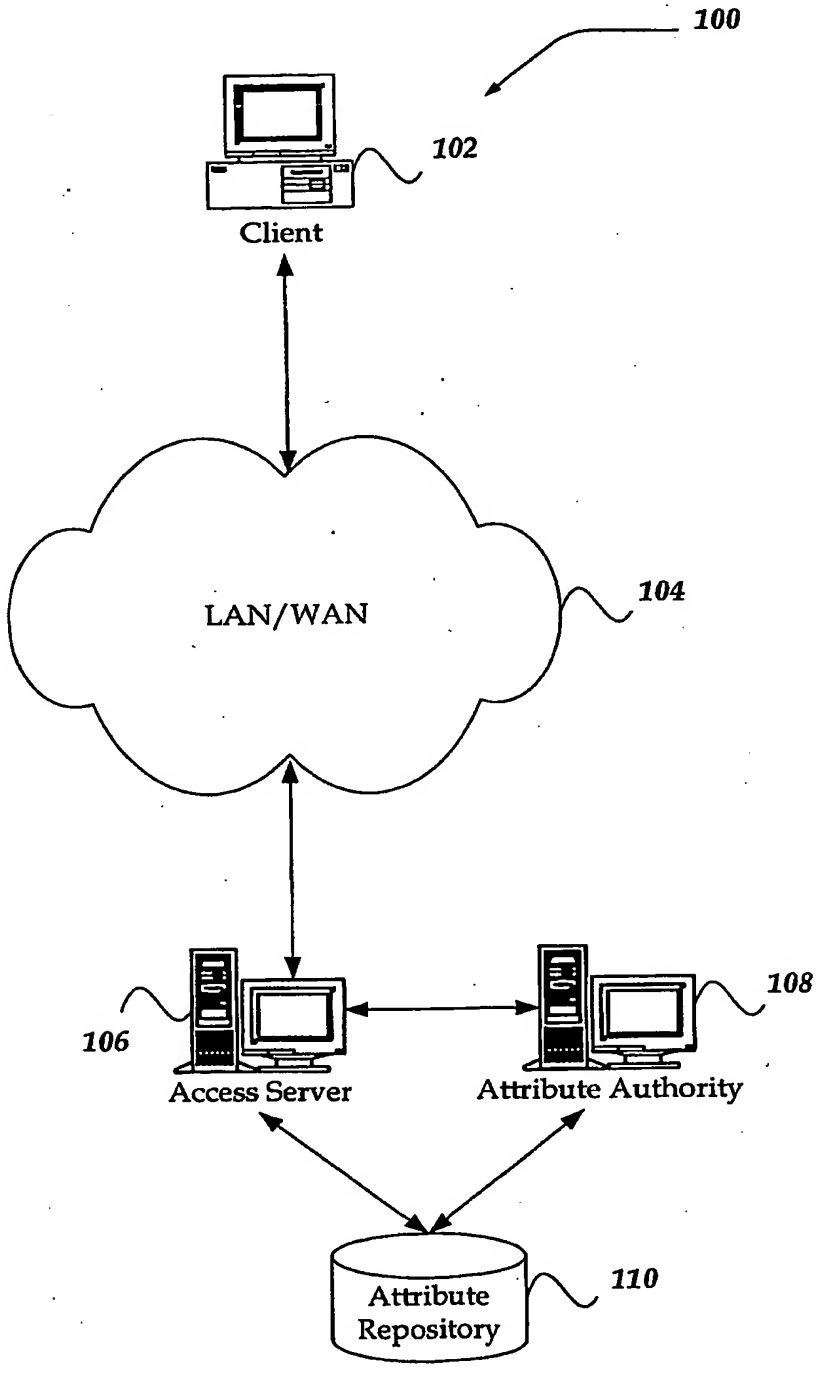
100
102
Client
LAN/WAN
104
106
Access Server
108
Attribute Authority
Attribute Repository
110

FIG. 1

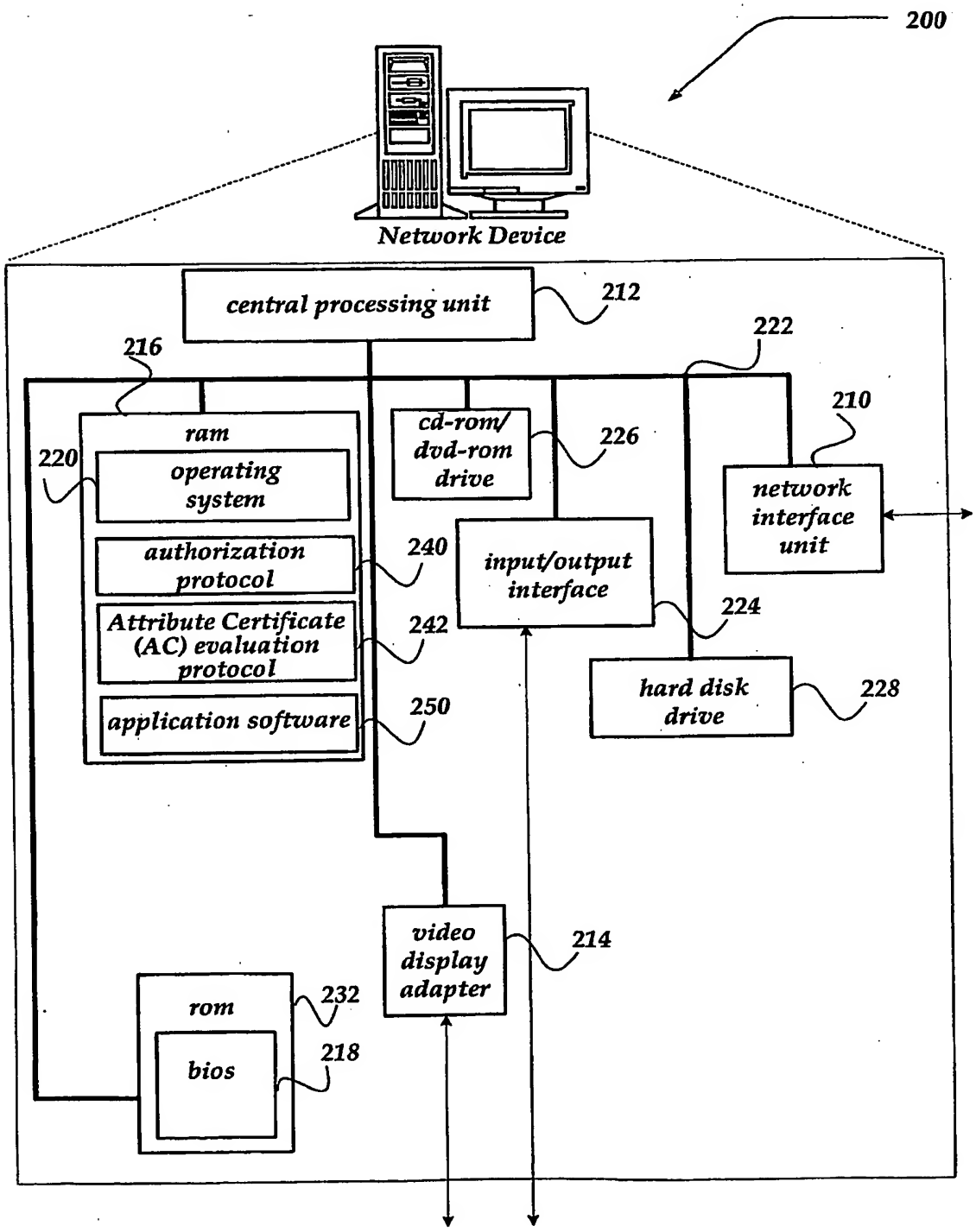
200
Network Device
central processing unit
212
216
222
210
ram
220
operating system
authorization protocol
240
Attribute Certificate (AC) evaluation protocol
242
application software
250
cd-rom/ dvd-rom drive
226
input/output interface
224
network interface unit
hard disk drive
228
video display adapter
214
rom
232
bios
218

FIG. 2

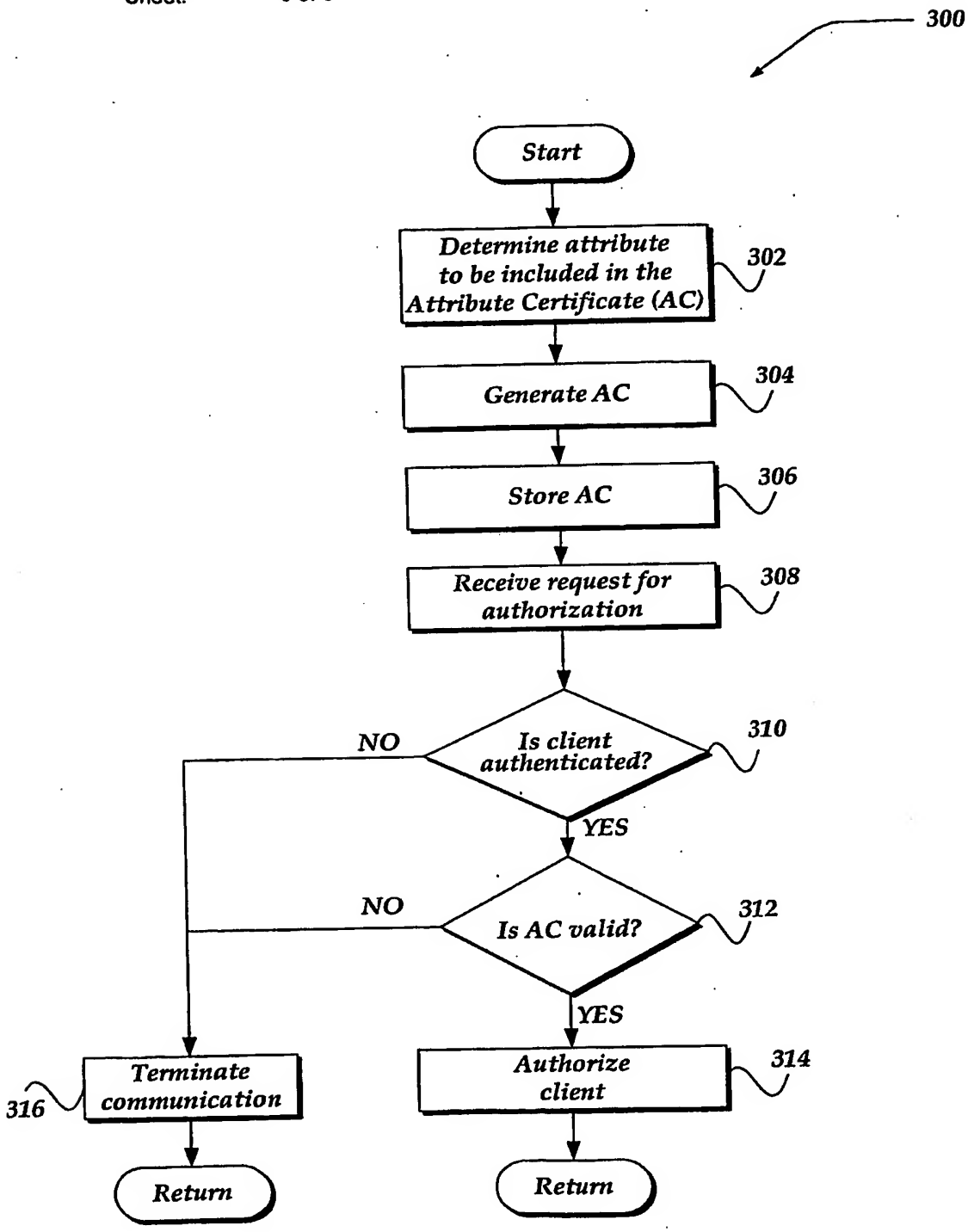
300
Start
Determine attribute to be included in the Attribute Certificate (AC)
302
Generate AC
304
Store AC
306
Receive request for authorization
308
Is client authenticated?
310
NO
YES
Is AC valid?
312
NO
YES
Terminate communication
316
Authorize client
314
Return
Return

FIG. 3

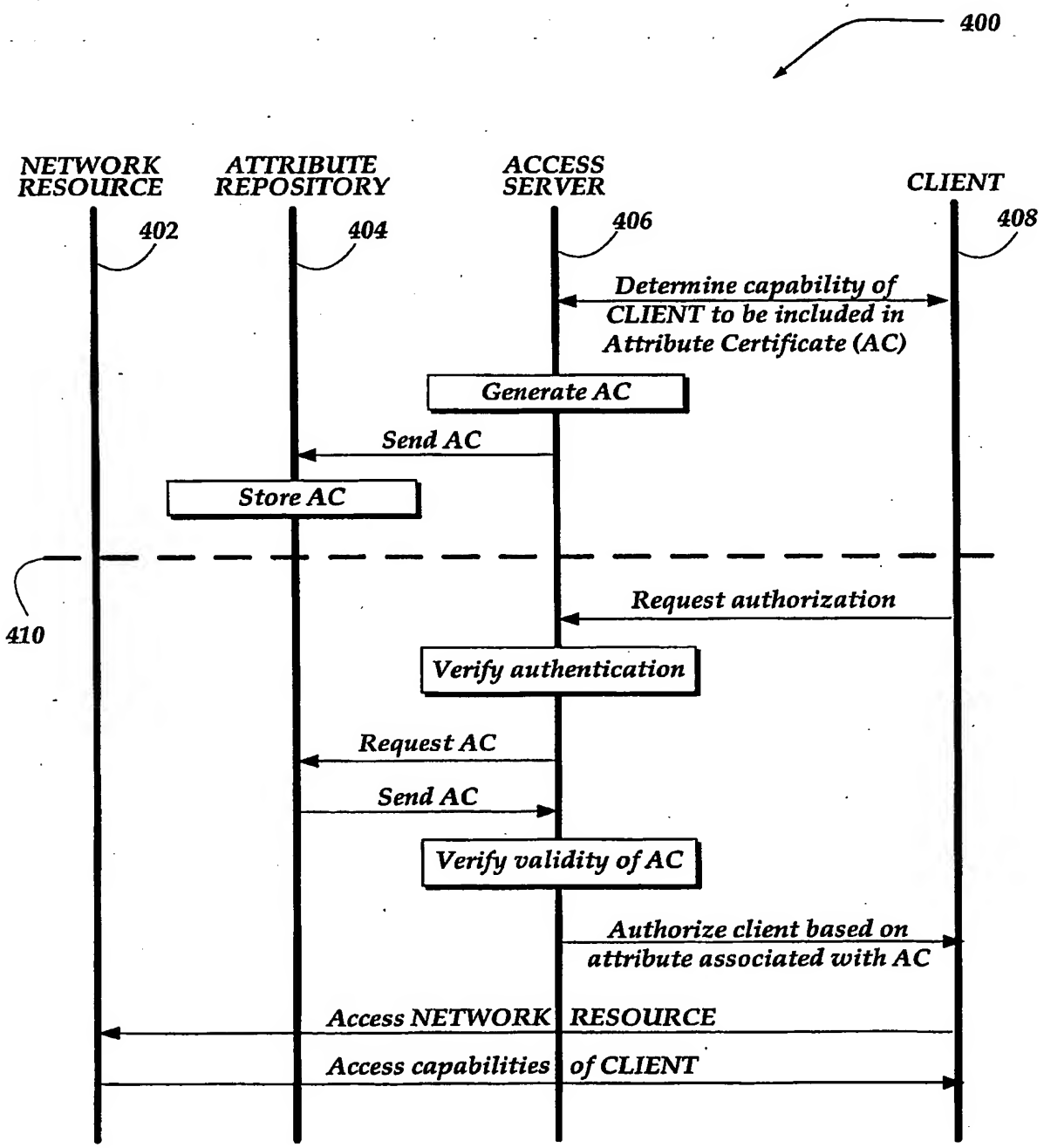

FIG. 4

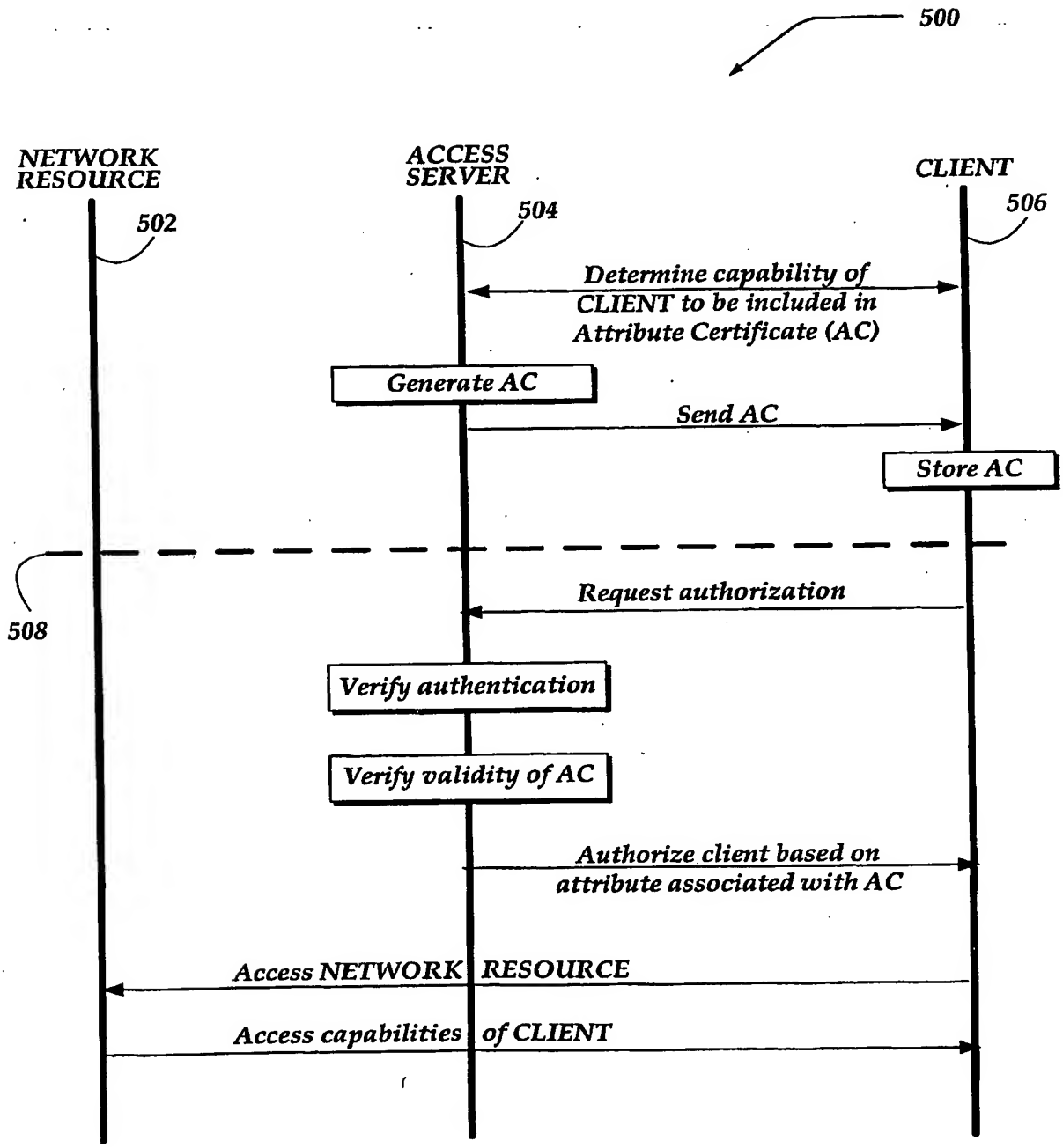
500
NETWORK RESOURCE
502
ACCESS SERVER
504
CLIENT
506
Determine capability of CLIENT to be included in Attribute Certificate (AC)
Generate AC
Send AC
Store AC
508
Request authorization
Verify authentication
Verify validity of AC
Authorize client based on attribute associated with AC
Access NETWORK RESOURCE
Access capabilities of CLIENT

FIG. 5

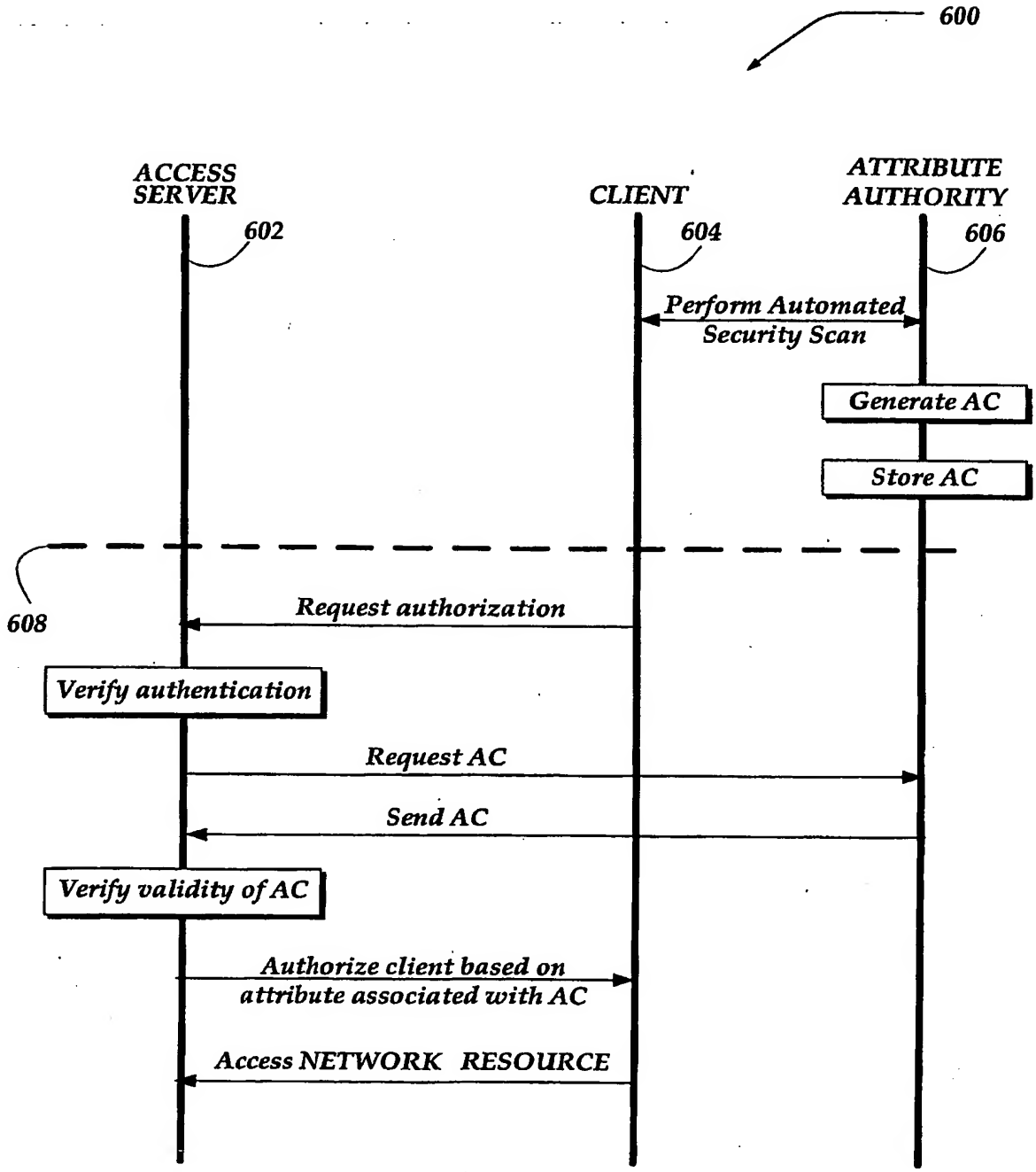

FIG. 6

Application Data Sheet

Application Information

Application Type::	Regular
Subject Matter::	Utility
Suggested Group Art Unit::	N/A
CD-ROM or CD-R?::	None
Sequence submission?::	None
Computer Readable Form (CRF)?::	No
Title::	SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES
Attorney Docket Number::	08212/0200353-US0
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	6
Small Entity?::	No
Petition included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Adam
Family Name::	Cain
City of Residence::	Madison
State or Province of Residence::	WI
Country of Residence::	US
Street of mailing address::	461 N. Few St.
City of mailing address::	Madison

State or Province of mailing address::	WI
Postal or Zip Code of mailing address::	53703

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Craig
Middle Name::	R.
Family Name::	Watkins
City of Residence::	State College
State or Province of Residence::	PA
Country of Residence::	US
Street of mailing address::	1883 Huntington Lane
City of mailing address::	State College
State or Province of mailing address::	PA
Postal or Zip Code of mailing address::	16803-3346

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Jeremey
Family Name::	Barrett
City of Residence::	Sugar Land
State or Province of Residence::	TX
Country of Residence::	US
Street of mailing address::	3330 Big Horn Ct.
City of mailing address::	Sugar Land
State or Province of mailing address::	TX
Postal or Zip Code of mailing address::	77478

Correspondence Information

Correspondence Customer Number::	38879

Representative Information

Representative Customer Number::	38879

Assignee Information

Assignee name::	Nokia, Inc.
Street of mailing address::	6000 Connection Drive
City of mailing address::	Irving
State or Province of mailing address::	TX
Postal or Zip Code of mailing address::	75039